IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF: THE RESIDENCE LOCATED AT 141 VICTORIA COURT LENOIR, NORTH CAROLINA 28645	Case No. 3:20-mj-00365 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jacob R. Guffey, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am investigating the activities of the social media account belonging to Dakota Ray MADDY, 141 Victoria Court, Lenoir, North Carolina (NC), 28645 (SUBJECT RESIDENCE). As will be shown below, there is probable cause to believe that MADDY used his social media account to transport, receive, possess, and distribute child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1), (a)(2) and (a)(5)(b). I submit this Application and Affidavit in support of a search warrant authorizing a search of the SUBJECT RESIDENCE as further described in Attachment A. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation, receipt, possession, and distribution of child pornography. I request authority to search the entire premises, including the residential dwelling, vehicles, located on the property, or any outbuildings such as detached garage, sheds, or barns. In addition, I request authority to search any computer and computer media located therein where the items specified in Attachment B, may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

2. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation (FBI), and have been so employed since April, 2008. I am currently assigned to

the Charlotte Division, Hickory Resident Agency. In this capacity, I am assigned to investigate cases involving child pornography, corporate fraud, public corruption, and similar violations. From 2012 to 2015, I worked on the Navajo Indian Reservation, in the Albuquerque Division, Gallup Resident Agency. At that assignment I conducted and participated in numerous death investigations, child sexual assaults, and other federal crimes occurring with the boundaries of Indian Country. From 2008 to 2012 I investigated Health Care Fraud in the Miami Division. I have personally been the case agent for numerous investigations that have resulted in the indictment and conviction of numerous subjects. I have also participated in the ordinary methods of investigation, including but not limited to, consensual monitory, physical surveillance, interviews of witnesses and subjects, and the use of confidential informants. I am an active member of the Evidence Response Team. Accordingly, I have executed numerous search warrants and seized evidence. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by 18 U.S.C § 3052 to conduct investigations of, and to make arrests for, violations of federal criminal statutes.

4. The facts set forth in this Affidavit come from my personal observations, my training and experience, evidence gathered pursuant to subpoenas, government records requests, and information obtained from other agents and witnesses. Because this Affidavit is submitted for the limited purpose of establishing probable cause to support the contemporaneously filed Applications, it does not include each and every fact known to me or to other investigators.

5. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of the violation of

Title 18 U.S.C. § 2252A, transportation, access with intent to view, possession, receipt, and distribution of child pornography are presently located at SUBJECT RESIDENCE.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of Title 18, U.S.C. § 2252A(a)(1), (a)(2) and (5)(B), relating to material involving the sexual exploitation of minors.

a. Title 18, U.S.C. § 2252A(a)(1) makes it a crime to knowingly mail, or transport, or ship, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, any child pornography.

b. Title 18, U.S.C. § 2252A(a)(2) makes it a crime to knowingly receive or distribute (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, U.S.C. § 2252A(5)(B) prohibits knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, video tape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes

any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. Like a phone number, no two computers or network of computers connected to the internet are assigned the same IP address at exactly the same date and time. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Based on my knowledge, training, and experience, I know that computer storage devices, such as a computer hard drive, can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

17. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

18. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, deleted, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware

drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

21. It is my experience with similar cases that individuals who download, produce, and/or distribute child pornography, often collect those files. The individuals who collect and produce child pornography store it on their electronic devices so that they may view it later. They also collect it so they may have something to use as barter for additional child pornography on the internet.

22. *Forensic evidence.* As further described in Attachment B, this Application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that

log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Background on LiveMe

25. According to information publicly posted on their website, LiveMe is a free mobile application that can be downloaded on mobile devices or accessed on their website in a limited fashion. It permits users to stream live video of themselves to an audience of fellow LiveMe users. Users can post comments and interact with people in the video (*e.g.*, give instructions or comments to other users). Users can also create or join groups where like-minded individuals can chat or message other users, post videos, images, text, and in this case, Uniform Resource Locators–known as URLs or "links"–directing users to Internet websites. Each LiveMe account has a screen name which can be changed by a user at any time. Screen names are displayed along with a unique "SID" number on a user's profile page. The screen name and SID are publicly visible to other users. The user's SID remains the same even when a screen name is changed.

26. Based on a review of company policy documents, including the company's privacy policy, along with information provided by other law enforcement officers, I know that LiveMe collects certain content created by users such as: subscriber/registration information; user posts such as images, video, audio, and text-based communications; data associated with user posts, videos, messaging (including voice and video), or other communications; and information about how users connect to LiveMe, such as IP addresses and certain device information. Based on other agents' experiences in similar investigations, I am aware that LiveMe maintains the content of chats, images, and videos sent between users.

27. In general, providers like LiveMe America, Inc. collect and ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include IP logs, device information, and other records that may tend to identify an individual such as email addresses, phone numbers, location data, or user-provided profile information.

28. Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

29. Finally, I am aware from my training and experience that electronic service providers such as LiveMe may report illegal conduct on their platform, specifically conduct related to the sexual exploitation of children, to the National Center for Missing and Exploited Children under the requirements of 18 U.S.C. 2258A. These reports, known as Cyber Tipline Reports, may contain information identifying a user, images, video, and/or text posted by a user on the company's servers in violation of terms of service and the law.

PROBABLE CAUSE

30. On July 8, 2020, the Honorable United States Magistrate Judge David Keesler signed a search warrant to obtain LIVEME account owner information, as well as evidence of violations of the aforementioned Title 18, U.S.C. § 2252A. Case number 3:20mj182 was assigned to that search warrant.

31. In summary, the Probable Cause statement outlined how a LiveMe user JSTEVENS2018,("TARGET ACCOUNT") had communicated with two separate undercover Agents in LiveMe chat rooms where users were known to distribute child pornography. During the chat sessions the TARGET ACCOUNT solicited child pornography as well as provided links which pointed to files containing child pornography. Those links were reviewed by investigators. Descriptions of their contents were provided in the previous Affidavit.

TARGET ACCOUNT INTERACTION WITH AN UNDERCOVER AGENT FBI DIVISION 1

32. On or about June 6, 2019, an undercover FBI Special Agent, FBI DIVISION 1, ("UC1") used the LiveMe service to access a group chat ("GROUP 1"). The UC1's activities were video recorded. Your Affiant has reviewed the video recording. Many of the posts overtly or obliquely referred to child pornography or the sexual exploitation of children. The UC1

observed GROUP 1 had several active users including user JSTEVENS2018, the TARGET ACCOUNT. The UC1 observed that users in GROUP 1 posted, distributed, and commented on child pornography, including multiple video files depicting the sexual exploitation of children, including infants and toddlers.

33. Beginning on or about June 09, 2019 and continuing through on or about June 10, 2019, the UC1 contacted the TARGET ACCOUNT, and the following chat occurred:

> UC1 statement to the group: I have about 1000 vids between the links I have. I'm sure there is stuff there lol", "I will send but not all for free lol", "need stuff in return"
> UC1: Hey I'm a 38 yo dad with a 9 year old daughter, no limits, USA hbu?[1]?
> TARGET ACCOUNT: I'm 27 no kids yet
> TARGET ACCOUNT: USA also
> TARGET ACCOUNT: No limits harder the better
> TARGET ACCOUNT: Hello?
> UC1: Hey are u active with any
> TARGET ACCOUNT: No sorry I'm not, U"
> UC1: Yes dau[2]
> TARGET ACCOUNT: Nice, every play with her?
> UC1: Yes
> TARGET ACCOUNT: Mmmm how old?
> UC1: She's 9
> TARGET ACCOUNT: Awesome such a great age, so active, pic?
> UC1: I'm open to sharing, just have to trust people. What the youngest u have, looking for OC[3], yunger the better
> TARGET ACCOUNT: I prefer 0-10 and kinda chubby lol I have about 1000 vids on different links
> UC1: Mmmm, Original Content?
> TARGET ACCOUNT: I wish I lost all my stuff when my computer went down a few months ago. I've been looking for a female like me to be with but it's impossible apparently
> UC1: Yes it is, well I like 0-10, let me know when u have really good stuff
> TARGET ACCOUNT: I have links
> UC1: Give me a sample of your best link
> TARGET ACCOUNT: My best one? I'll send a link yea. What you sending?
> UC1: I have a sample I can send of my dau, but u have to delete
> TARGET ACCOUNT: Okay, I always do especially when it's family

[1] A common abbreviation online for "how 'bout you?"
[2] A common abbreviation online for "daughter"
[3] A common abbreviation online for "Original Content"

TARGET ACCOUNT: *[A Service 1 "link" was sent containing numerous videos of child pornography, depicting nude prepubescent age girls masturbating, engaging in sex acts with other children, and posing in sexually explicit positions.]*
TARGET ACCOUNT: Now u?

34. The link sent to UC1 from TARGET ACCOUNT directed to SERVICE 1, a foreign-based file hosting service. From my training and experience, including experience with recent investigations, I am aware that SERVICE 1 is commonly used by child pornographers and persons seeking to receive and distribute child pornography. SERVICE 1 allows people to share files that are stored on SERVICE 1's servers and not directly on a user's computer. In the context of GROUP 1 it would be expected by other users that the TARGET ACCOUNT's links would direct to child pornography.

35. The UC1 accessed the link and found that it directed to a folder titled, "Girls," which contained approximately 4.16GB of data. The folder contained approximately 175 files—almost all of which were video files, and many of which had titles indicative of child pornography. These titles included terms such as: "7yo[4] girl shows pussy & ass in front of sleeping…;" "11yo Dance Strip Spread", and "12yo cutie pops out her swollen clit". Most of the files listed had a preview or thumbnail image next to the title. Many of the preview images depicted females who appeared to be under the age of 12, who were engaged in sexually explicit conduct, or whose genitalia were the focal point of the image. UC1 did not view or download the videos.

36. The UC1 accessed the user's profile page. On or about June 9, 2019, the TARGET ACCOUNT's profile listed a location of "outerspace." The account had 58 "fans" and followed 226 other accounts.

[4] A common abbreviation for "years old."

TARGET ACCOUNT INTERACTION WITH AN UNDERCOVER AGENT FBI DIVISION 2

37. On or about April 22, 2020, an undercover FBI Special Agent, FBI DIVISION 2, ("UC2") used the LiveMe service to access a group chat ("GROUP 2"). The UC2's activities were video recorded. I have reviewed the video recording. Many of the posts obliquely referred to child pornography or the sexual exploitation of children. The UC2 observed GROUP 2 had several active users, including user JSTEVENS2018, the TARGET ACCOUNT. GROUP 2's title implied the content therein was meant to be sexually perverted. The UC2 observed that users in GROUP 2 posted links to Service 1.

38. The UC2 observed that the user of the TARGET ACCOUNT posted one link in GROUP 2. The link directed to SERVICE 1. In the context of GROUP 2, and GROUP 2's title, it would be expected by other users that the TARGET ACCOUNT's links would direct to child pornography.

39. The UC2 accessed the link and found that it directed to a folder titled, "Solo,". The folder contained approximately 423 video files, some of which had titles indicative of child pornography. These titles included terms such as: "pornstarbaby1" and "sexybaby". The files viewable to UC2 had a preview or thumbnail image next to the title. Many of the preview images depicted females who appeared to be under the age of 12, and who appeared to be engaged in sexually explicit conduct.

40. UC2 accessed a video file titled "2018-12-29 11.43.52.mp4". The file depicted a female approximately 15 to 20 years of age holding a minor female approximately 8 to 11 years of age. The minor is seen completely naked with the genitalia directed toward the camera. The older female is seen rubbing the child's labia.

41. After posting the link, the TARGET ACCOUNT asked, "Anyone sharing?" After that request was made, another user posted several links. The UC2 accessed a link posted by this user, which was available to the TARGET ACCOUNT. The link directed the UC2 to SERVICE 1. The file, named, "Kamilla (Camilla)", contained approximately 459 video files, some of which had titles indicative of child pornography. These titles included, "!New! (Pthc[5]) Daddy…" and "(PTHC LOLIFUCK OP…[6])". Many of the preview images depicted females who appeared to be under the age of 12, and who appeared to be engaged in sexual activity. Your Affiant recognized several of the videos, from previous investigations, as video files containing child pornography, including:

a. A video file with a run time listed as 2:17, titled, "(NEW)_20101002_Fu…" The video was not accessed by UC2, however, your Affiant recognized the thumbnail image as previously identified child pornography. The thumbnail is of a completely nude female under the age of 8, with an adult male's penis in her vagina and the words "FUCK ME" written on her stomach, with an arrow pointing to her vagina.

42. On May 9, 2020, UC2 encountered TARGET ACCOUNT on LiveMe, in GROUP 3 chat, where TARGET ACCOUNT was the group owner. TARGET ACCOUNT wrote, "Welcome everyone share please". The UC2's activities were video recorded. Your Affiant has reviewed the video recording. Many of the posts overtly or obliquely referred to child pornography or the sexual exploitation of children. The UC2 observed GROUP 3 had an active user who posted approximately 7 links to Service 1 with a total size of approximately 58.3GB. One of the 7 links returned a message that the account had been removed for "objectionable

[5] "PTHC" is a common term known to mean Pre Teen Hard Core
[6] "LOLI" is a term used to mean a minor female

content, such as Child Exploitation Material". After the links were posted, TARGET ACCOUNT replied, "Anything new? Those have been around a while."

43. The UC2 accessed the files associated with the shared links. Your Affiant viewed the files and has provided the following summaries of videos which TARGET ACCOUNT had access to:

a. "9yo handjob cumshot on hand.mp4", is a video file approximately 56 seconds long. In the video a female, who is nude from the waist down, and who appears to be under the age of 8 assists an adult male in masturbation while holding his penis.

b. "VID-20151105-WA0015.mp4", is a video file approximately 51 seconds long. In the video, an adult male has his erect penis in the anus of a female who appears to be under the age of 12, and who is nude from the waist down.

44. GROUP 3's title implied the content therein was meant to be sexually perverted.

45. Your Affiant is aware from his training and experience that individuals with a sexual interest in children and child pornography often seek to satisfy that interest through the acquisition of sexually explicit depictions of children. Possession of sexualized, but non-pornographic depictions of children—referred to herein as child erotica–may also indicate a sexual interest in children. Additionally, because child pornography imagery is often focused on the lower half of the child's body and the child's face may not be visible in all images of a series, child erotica images—such as the depiction of partially dressed or undressed child victims—are often helpful in identifying victims and locations where children may have been victimized.

IDENTIFICATION OF THE ACCOUNT USER

46. On or about October 11, 2019 LiveMe provided information in response to a subpoena related to the TARGET ACCOUNT. LiveMe records show the account is associated with SID 243159058. The account was registered on an iPhone 11, iPhone XS Max Global smartphone. The account was associated with EMAIL ADDRESS 1. IP Address: 47.38.87.78 was used to access the account resolved to Charter Communications on or about September 13, 2019.

47. On or about October 16, 2019 Charter Communications provided information in response to a subpoena related to the IP Address described in paragraph 46. The account was registered to Jenniffer Maddy, 141 Victoria Ct, Lenoir, NC, 28645.

48. The user of TARGET ACCOUNT appeared to be located within the Western District of North Carolina when they distributed and attempted to distribute child pornography to the UC1, UC2, and others.

49. On or about August 6, 2019 Google provided information in response to a subpoena related to EMAIL ADDRESS 1. The name on the account was Josh Stevens. The account was created on March 24, 2018. The telephone number associated with the account was 817-403-5009.

50. On or about September 3, 2019 Verizon provided information in response to a subpoena related to telephone number 817-403-5009. The phone number was registered to Cassandra Williams, 128 Freese Dr, Sanger, TX, 76266.

51. Open source database checks showed Cassandra Williams was associated with 128 Freese Dr, Sanger TX, 76266 as well as 209 Marion Dr, Little Elm, TX, 75068. Open source

database checks showed that MADDY was also associated with those addresses. Your Affiant is aware that MADDY pays child support.

52. A review of materials received from the search warrant served to LiveMe returned the following new information:

a. From about June 8, 2019 through about May 12, 2020 the TARGET ACCOUNT accessed the internet through various IP addresses associated with an ATT Wireless account. The states associated with the accounts, according to the LiveMe production, were associated with Texas, California, Georgia, Maryland, and Michigan. Your Affiant served ATT Wireless with a subpoena requesting account subscriber information. ATT replied that information related IP addresses associated with cellular telephone use was not maintained and therefore could not be provided to your Affiant.

b. On or about May 6, 2020, the TARGET ACCOUNT accessed the internet through a Spectrum Business account. In response to a subpoena, Spectrum identified the account as belonging to Danny Herman, 15622 Valley Blvd, Fontana, California, 92335. An open source search of this address showed it belonged Danny Herman Trucking.

c. An open source search of Danny Herman Trucking produced two company newsletters listing MADDY as an employee. Danny Herman Trucking listed its home office address as 339 Cold Springs Rd, Mountain City, TN, 37683.

d. As of November 19, 2020, your Affiant was aware that MADDY lived at SUBJECT ADDRESS with his mother, Jenniffer Maddy and his father. Your Affiant was aware that MADDY worked from 5:00am until 5:00pm.

53. The LiveMe search warrant showed the TARGET ACCOUNT was accessed through an iPhone 11,6 from June 8, 2020 through May 12, 2020.

CONTINUED ACTIVITY

54. On or about December 8, 2020, LiveMe responded to a subpoena requesting current subscriber information for TARGET ACCOUNT for activity which occurred between September 2, 2020 and November 19, 2020. LiveMe provided the following updated information:

a. IP address 65.132.137.174 was last used to access the account on or about October 26, 2020.

b. IP address 47.38.80.174 was last used to access the account on or about November 11, 2020.

c. IP address 47.135.67.64 was last used to access the account on or about October 26, 2020.

d. Several IP addresses were returned which came back to AT&T Mobility. Your Affiant is aware that AT&T does not maintain records for dynamic IP addresses.

e. Device ID: LM:JAaJr3+QemeXCsK+EMnSKRyOi+v3Gwtlk73fzVUd1M=

f. Device Model: SM-G988U

55. On December 17, 2020, Charter responded to a subpoena request for subscriber information for IP addresses 47.135.67.64 and 47.38.80.174 for the aforementioned dates and times. The subscriber information returned was for:

a. Subscriber Name: Jenniffer Maddy

b. Subscriber Address: 141 Victoria Ct, Lenoir, NC, 28645

56. On December 14, 2020, Century Link replied to a subpoena which had been previously served to Qwest, which is owned by Century Link. They advised the IP address, 65.132.137.174 was being used by CVB, doing business as Malouf, located in Lenoir, North Carolina.

CONCLUSION

57. Based on the aforementioned information, your Affiant respectfully submits that there is probable cause to believe that MADDY acted through TARGET ACCOUNT to transport, receive, posses, and distribute child pornography. Your Affiant respectfully submits that there is probable cause to believe that MADDY has violated 18 U.S.C. §§ 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2) and (a)(5)(B), is located in the SUBJECT RESIDENCE described in Attachment A, and this evidence, listed in Attachment B to this Affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

Respectfully submitted,
s/ Jacob R. Guffey
Special Agent Jacob R Guffey
United States Department of Justice
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 23rd day of December, 2020, at 1:10 PM

Signed: December 23, 2020

David S. Cayer
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The residence, outbuildings, structures, appurtenances, and vehicles located at 141 Victoria Court, Lenoir, North Carolina, 28645. The residence is described as a single story home with red brick. It has a paved driveway and also a chain linked fence. There is a mailbox with the house number and the name Maddy on it.

ATTACHMENT B

Particular Things to be Seized

1. Instrumentalities of the violations contained within the Application for the search warrant at 141 Victoria Court, Lenoir, North Carolina, 28645:

a. any computer, computer system, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, hard drive and other computer related operation equipment, photographs and other visual depictions of such graphic interchange formats (JPG, GIF, TIF, AVI, and MPEG), electronic data storage devices (hardware, software, diskettes, backup tapes, CDs, DVD, flash memory devices, thumb drives, and other storage media); and any input/output peripheral devices, passwords, data security devices, and related security documentation;

b. books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A);

c. originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A); and

d. motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A).

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet;

4. Any child pornography as defined by 18 U.S.C. § 2256(8);

5. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence;

6. Documents and records regarding the ownership and/or possession of the searched premises;

7. Credit card information, bills, and payment records;

8. Information or correspondence pertaining to affiliation with any child exploitation websites;

9. Any material that is "child erotica";

10. Any correspondence/records indicating the true identity of any member or user of "LiveMe" and;

11. Any correspondence, e-mails, electronic messages, and records pertaining to "LiveMe"

As used above, the terms "records" and "information" refer to all forms of creation or storage, any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, videotapes, motion pictures, or photocopies).

The term "computer" refers to all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions: desktop computers, notebook computers, mobile phones, tablets, server computers, smart phones, and network hardware.

The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples are hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of

the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.*, the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.